# Assessing the Vulnerability of Infrastructure Networks based on Distribution Measures

Giulio Galvan, Jitendra Agarwal*

Department of Civil Engineering, University of Bristol, University Walk, Bristol, BS81TR, UK

*: Corresponding Author: Jitendra Agarwal, J.Agarwal@bristol.ac.uk

**Highlights**

A distributional metric for infrastructure vulnerability is proposed.

Its effectiveness is illustrated through power, transport and water supply networks.

Uncertainty in the vulnerability assessment of high-order disruption scenarios is quantified.

Vulnerability analysis framework is formalised.

## ABSTRACT

Infrastructure networks enable communities to be resilient by distributing essential services and supporting the relief and recovery actions necessary to bounce back from disruptive events. In order for infrastructures to play this central role, their own vulnerability needs to be assessed and managed. In this paper, a new distributional metric for vulnerability assessment is presented. Unlike existing methodologies, it aims at producing a characterisation of infrastructure vulnerability which accounts in full for the variability of the service delivery performance across disruption scenarios. The applications of the metric to theoretical configurations as well as real infrastructure networks are exemplified. These examples demonstrate that the proposed metric enables transparent and comprehensive information on the vulnerability of infrastructure networks. It is noted that the use of average values of system performance under different disruption scenarios may lead to unsafe conclusions about the system vulnerability. The proposed approach is also able to quantify the uncertainty in the vulnerability assessment of high-order scenarios. The paper also shows how the formalisation of the building blocks of vulnerability analysis made here, unifies many of the other methodologies found in the literature.

**Keywords**: Disruption Scenarios, Infrastructure Systems, Networks, Vulnerability Analysis

## 1. INTRODUCTION

Infrastructure systems form the backbone of modern societies. Communities, businesses and governments all rely on the continuous supply of services such as energy, water, and transportation services (1). These systems are organised in networks of multiple interdependent elements, none of which is valuable *per se*, but depends on the interactions with other elements of the same network (and of other networks) in order to deliver its service to society (2). Reliable infrastructure networks foster the prosperity of communities during their normal operations (3) and, when these communities suffer from natural or man-made hazards (e.g. earthquakes, floods or terrorist attacks) infrastructures play a central role in the resilience process (4) by supporting response and recovery activities.

For infrastructures to fulfil this role, it is necessary to reduce their own vulnerability to internal and external hazards. Vulnerability is defined as susceptibility to damage or more formally as "the degree a system is affected by a risk source or agent" (5). Such definition is specified here for infrastructure systems as "the degree of reduction in the service delivery capacity of the infrastructure after a disruption". A vulnerability assessment of an infrastructure system requires the exploration of its performance under a wide array of disruptive events and in the literature several examples of vulnerability analysis of infrastructure networks can be found, e.g. (6), (7) or (8). It is important that infrastructure networks are made robust against known hazards as well as unknown hazards and to that end, complementing quantitative risk analyses of probable scenarios with the exploration of low-probability, high-consequence scenarios is a necessity given the pivotal role infrastructures play in the well-being and prosperity of communities.

This paper provides a distributional metric for vulnerability assessment which can be used, with appropriate adaptations, on any infrastructure organised as a network. While facilitating the exploration of the behaviour of the system independently of the hazard identification, this approach allows for the discussion of three aspects of vulnerability analysis which are commonly neglected: (i) what constitutes a reference model for the vulnerability of infrastructure networks, (ii) how incomplete the information provided by the analysis is and (iii) what robustness is associated with the simulation of a number of disruption scenarios which is necessarily smaller than a complete set of scenarios by orders of magnitude.

This paper is organised as follows: Section 2 provides a critical review of vulnerability analysis of infrastructure networks; Section 3 formalises a vulnerability analysis framework; Section 4 presents the proposed distributional

metric for vulnerability evaluation and exemplifies this with application to networked infrastructures; Section 5 elaborates the novel features of the metric and considers application of high-order scenarios to real networks; Section 6 provides a critical discussion of the approach and how it links to existing methodologies. Conclusions are drawn in Section 7.

## 2. VULNERABILITY OF INFRASTRUCTURE NETWORKS

The need to ensure the continued operation of infrastructure networks has been recognised by academics (9), governmental agencies (10) and NGOs (11). Yet, because of the multiplicity of the assets required to ensure a thorough delivery of service (2) and the uncertainty around the natural and man-made hazards to which they are exposed (12), conventional risk and reliability analyses only provide part of the information necessary to manage these complex systems (13). These analyses identify the hazardous events with the potential to initiate failure processes (hazard analysis) or assign failure likelihoods to the system elements in order to compute (analytically or numerically) the possible system-level disruptions and the associated probabilities (reliability analysis). The outcome of risk and reliability analyses adequately characterises the performance of a network subject to a limited number of failure events, but fails to thoroughly explore low-probability, high-consequence scenarios (14). These scenarios are particularly important if they are associated to high-magnitude hazardous events, because they will also cause the most damage to the communities that depend on the infrastructure. In other words, an infrastructure vulnerable to these events may be a hindrance for the resilience of the communities it supports. Vulnerability analyses have been devised in order to characterise the behaviour of the system in such high-consequence scenarios independently of the likelihood of the initiating event(s) (15).

The vulnerability analysis of networks has its conceptual roots in the percolation analysis of graphs, a field which has been studied in mathematics and statistical physics over the last few decades (16) (17) (18). Percolation analysis is concerned with the identification of the fraction of nodes, the percolation threshold, that need to be removed from a network in order for its giant component to disappear. More recently, the percolation of coupled networks has been studied (19), in order to understand the behaviour of interdependent networks, as well as the percolation of spatial networks (20), which model more closely real world infrastructure networks. When applied to engineering, the thrust of the analysis changes from assessing the percolation threshold to quantifying the impacts arising from the removal of any set of nodes. While connectivity has maintained its role for the quantification of the

impact of adverse events (21), more elaborate topological functions have been used, such as the average size of the disconnected clusters (22), the increase in the average path length of the network (23) or the loss in network efficiency (24). Further, functions measuring the service delivered by the infrastructure network have been devised. These range from topologically-based flow metrics to higher fidelity functions based on modelling of the physical behaviour of the network (25). While the latter are preferable in theory, they come at a computational cost greater by orders of magnitude (8), which makes them prohibitive for vulnerability analyses where a large number of different scenarios need to be simulated. Vulnerability analyses have been performed on infrastructure networks of different sizes and belonging to diverse technological domains (26). The following provides across-section of the body of work on the vulnerability of infrastructure networks.

Electric power networks represent the prime example of infrastructure analysed from a vulnerability perspective. The development of vulnerability analysis was driven in this field by large-scale unexpected events that affected these networks, e.g. the Northeastern blackout which affected the US power grid in 2003 (27). Such dramatic phenomena are driven by the possibility of cascading failures, and can be modelled (28) using an alternate current power flow model. This model, however, is computationally intensive, requiring the solution of large systems of nonlinear equations. Simplified models have thus been used: for example, the Motter and Lai model (29) was used to assess the loss of connectivity arising from failures cascading through the Italian electric power transmission network (30), and the ORNL-PSerc-Alaska model (31) was used to evaluate the loss in efficiency associated with disruptions to the French electric power transmission network (32).

Transport networks of multiple types have also been examined under the lens of vulnerability. The European Air Transportation network was assessed for its vulnerability to spatially-localised disruptive events in the aftermath of the Eyjafjallajökull volcano eruption in Iceland (33): it was found that this network is characterised by a spatially-definite pattern of vulnerability. A flood vulnerability analysis of the Chinese railway network (34) concluded that the key parameter governing the criticality of railway connections is the actual traffic flowing through them, rather than their exposure to flood hazards. A methodology for the assessment of the vulnerability of road networks to multiple hazards has been presented in (35).

The vulnerability of water and gas distribution networks has also been scrutinised with similar tools: the scale of these assessments varies widely, ranging from the Europe-wide model of the gas network (36) to the city scale

network of Kumasi in Ghana (37). Topological functions have been found to be effective at assessing the effects of node disruptions on the flow in water pipeline networks (38), and a model, based on the Motter and Lai dynamics, for simulating the vulnerability of pipeline systems to cascading failures has been proposed in (39).

The vulnerability of multiple interdependent networks has been the focus of a number of other papers (40), as the coupling between different infrastructure systems induces new, and sometimes surprising, failure mechanisms. For example, a methodology for the identification of the most critical elements as well as the fraction of elements that need to be removed in order for the system to completely lose its functionality, has been presented in (41). The coupling between water distribution networks and electric power systems in Shelby County, Tennessee, has been examined in (21) and (42). These concluded that the former shows higher vulnerability to disruptive events when the dependency on the latter is taken into account.

The focus of several other studies is on the vulnerability of infrastructure networks to specific hazards (e.g. floods (34), earthquakes (43) and hurricanes (44)). These works differ from the vulnerability analyses presented earlier only in the scenario generation phase. Nodes and edges are disconnected in the different disruption scenarios on the basis of the spatial distribution of the natural hazards and the fragility of the elements. Then, the consequences of such scenarios are assessed by computing their system-level impacts.

The works presented above (as well as many others not listed here) share the common objective of probing the behaviour of infrastructure networks subjected to external disruptions. The main steps required for this assessment are similar across vulnerability analyses performed on systems belonging to a variety of technological domains. However, there is a lack of a framework which explicitly states what these steps should be. These common steps are followed implicitly and only passing remarks are provided about the methodological underpinnings of these analyses. This hinders a transparent comparison among vulnerability analyses, which in most instances are actually comparable, differing only in some minor aspect. The outcome of these vulnerability analyses is also presented in a variety of formats, which further complicates the task of providing a comparison among their results. Finally, while simulation approaches are often used to probe the system states arising from disruptions (14) (45), a methodology to assess the robustness of these results, to the authors' knowledge, has never been proposed.

## 3. A VULNERABILITY ANALYSIS: BUILDING BLOCKS

The building blocks of a vulnerability analysis framework are represented graphically in Fig. 1 and discussed below. Steps 1 to 4 formalise the common practice for the vulnerability analysis of infrastructure networks, while Step 5 specifies the format of the results of a vulnerability analysis in order to prevent loss of information and assess the uncertainty about the outcomes of the simulations.

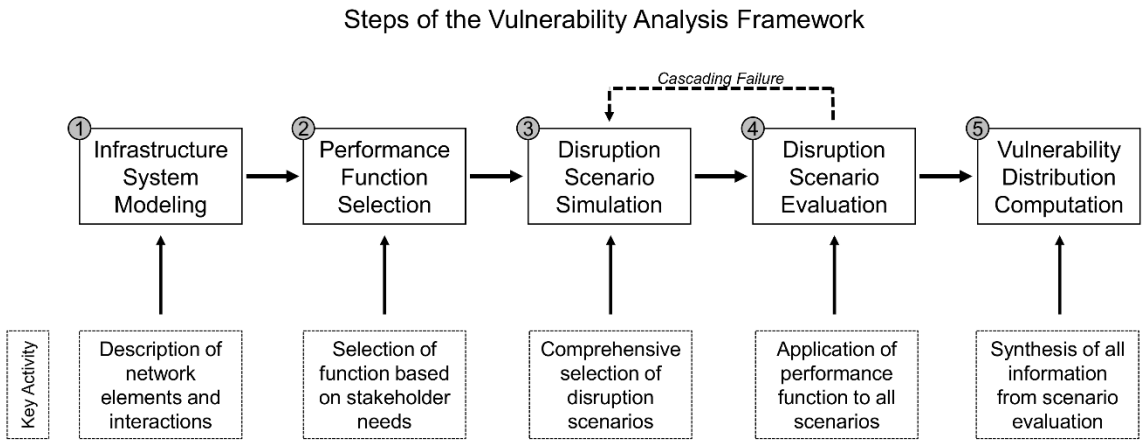


*Fig. 1. The building blocks of a vulnerability analysis framework.*

### 3.1. Infrastructure System Modelling

Vulnerability analysis builds on the mathematical modelling of the infrastructure under consideration. Multiple methodologies, such as Agent-Based Modelling or System Dynamics, have been used to capture different aspects of the behaviour of infrastructure systems (40), but the work presented here uses the network science paradigm. Such modelling aims to capture two defining features of infrastructure networks: (a) the multiplicity of the assets and their interconnections, and (b) the emergent property of the system which is its capacity to deliver service to the communities it supports.

*Table I: Examples of infrastructures modelled as networks in the scientific literature and characterisation of their nodes and edges*

| System | Nodes | Edges | Reference |
|---|---|---|---|
| Electric Power Transmission | Generators and Substations | Power Lines | (46) |
| Water Distribution | Pumping Stations, Storage Tanks | Pipelines | (47) |
| Natural Gas Distribution | Pumping Stations, Storage Tanks | Pipelines | (36) |
| Road Systems | Origins and Destination, Intersections | Road Segments | (48) |
| Railway Networks | Railway Stations | Railway Lines | (49) |
| Airport Networks | Airports | Flight Routes | (38) |

The infrastructure system is thus represented by a graph *G* which is the collection of two disjoint sets, the nodes $\mathrm{N}$ and the edges $\mathrm{M}$ (50). The cardinality of the node set is indicated by *n*, and the cardinality of the edge set is indicated by *m*. In this paper, a generic asset of a network, which can be a node or an edge, is defined as an element. In the network model, the nodes represent the infrastructural assets where the service is being generated, distributed, or delivered. The physical characterisation of the nodes varies among infrastructures. The edges represent the connections between the nodes. They are the channels through which the service is exchanged from node to node. The connectivity pattern of the system is represented by the *n*-by-*n* adjacency matrix $\boldsymbol{A}$ where every entry $a_{ij}$ maps the existence and the features of the edge between nodes *i* and *j*. Examples of modelling of infrastructure network elements are reported in Table I.

### 3.2. Performance Function Selection

The performance of the infrastructure network that is of interest in a vulnerability analysis is its service delivery capacity. This is a system-level property that emerges from the microscopic states of its elements and their interactions. While the interactions among the elements are mapped by the adjacency matrix of the system, it is necessary to define, for every element, an additional variable mapping its state. These are collected in system state vector $\boldsymbol{S}$: in the simplest version of vulnerability analysis, the states of the elements are defined in binary terms (i.e. the $i^{th}$ element is functional when $s_i = 1$ and the element is removed from the network when $s_i = 0$).

It is also necessary to establish a reference performance against which to compare the disrupted performance. The reference performance is evaluated on the undisturbed configuration of the system, which is characterised by vector $\boldsymbol{S_0}$ where $s_i = 1 \ \forall \ i$. This assumption is a simplification of reality, where neither minor malfunction of system elements need imply any service reduction nor the functional state of the system need to be the one where every element is working as intended. However, this assumption is used in much of the vulnerability literature to establish a reference point and this convention is adopted here. The service delivery capacity of an infrastructure system is assessed through the use of a system performance function *Q* which maps $\boldsymbol{S}$ to a real number:

$$Q: \boldsymbol{S} \rightarrow \mathbb{R} \tag{1}$$

$$Q: \boldsymbol{S} \mapsto f[\boldsymbol{A}(\boldsymbol{S}), \boldsymbol{X_1}, \dots, \boldsymbol{X_p}] \tag{2}$$

Equation (2) states that the outcome of a performance function $Q$ depends on the adjacency matrix $\boldsymbol{A}$, which in turn depends on the system state $\boldsymbol{S}$, and any additional variables (included in vectors $\boldsymbol{X_1, \ldots, X_p}$) required by the performance function. The multiplicity of stakeholders interested in the performance of the infrastructure implies that a variety of performance functions can be used to reflect their needs. Examples of performance functions used in the literature are reported in Table II, and they all represent in some way the ability of infrastructures to deliver service to society. For example, if the decision-maker is concerned with maintaining a set amount of service delivered through the network, functions able to compute its reduction (e.g. *B* or *F* in Table II) must be used. On the other hand, if the objective is an affordable service, then measures that account for its cost (e.g. *E*) are the most appropriate. Vectors $\boldsymbol{X_1, \ldots, X_p}$ are introduced to account for the additional information required to compute some of these functions. For example, the Service Delivered function *B* presented in Table II (and frequently used in vulnerability assessment of electric power systems) requires the definition of demand at distribution nodes, of supply at generation nodes, and of the capacity of nodes and edges.

*Table II: Examples of performance functions and the corresponding formula*

| Performance Function | Formula | Reference |
|---|---|---|
| Connectivity | $C = n_c/n$ | (42) |
| Network Efficiency | $E = \sum_{ij}(1/l_{ij})/n(n-1)$ | (32) |
| Service Delivered | $B = \sum_{i \in D} d_i - \sum_{i \in S} s_i$ | (25) |
| Functional Elements | $F = n_f/n$ | (51) |
| Algebraic Connectivity | $\Delta = \lambda_2$ | (37) |
| Well-formedness | $Q = \sum_{i \in c} \det(k_{ii})$ | (52) |

*Notation: $n$ = number of nodes in the network, $n_c$ = number of nodes in the giant component, $l_{ij}$ = length of shortest path among node $i$ and node $j$, $d_i$ = demand at node $i$, $D$ = set of demand nodes, $s_i$ = supply at node $i$, $S$ = set of supply nodes, $n_f$ = number of functional nodes, $\lambda_2$ = algebraic connectivity of the network, $k_{ii}$ = stiffness submatrix of node $i$, $c$ = set of nodes in the giant cluster*

### 3.3. Disruption Scenario Simulation

Disruptions are defined in terms of the individual states of the system elements, i.e. failures of nodes or edges or a combination of both. The state of their elements is represented here as binary: either they are functional or not functional. However, the approach can be generalised to account for discrete states of the system elements.

Disruption scenarios are categorised in the systems engineering literature by the number of contemporary element failures (e.g. (14), (53)). Scenarios involving the failure of *k* out of *N* = *n* + *m* system elements are denoted as *N* - *k* scenarios, where *k* is the disruption order. For every *k,* a disruption space $\boldsymbol{\Omega_{N-k}}$ can be identified. The disruption space $\boldsymbol{\Omega_{N-k}} = (\boldsymbol{\omega_1^{N-k}}, \boldsymbol{\omega_2^{N-k}}, \ldots, \boldsymbol{\omega_n^{N-k}})$ is the set of all the distinct disruption scenarios $\boldsymbol{\omega_i}$ involving *k* failures. It is a discrete set where every element is a perturbation of the system state vector with *k* null entries, and its cardinality is equal to the binomial coefficient $N_k = N!/(k!\,(N-k)!)$. Rather than generating disruption scenarios based on a specific hazard or selected perturbations, vulnerability analysis strives to probe the whole disruption space: this is critical to guard against low probability, high consequence scenarios. If a specific hazard is used to generate the disruption scenarios against which the system performance is assessed, the only information gained is its performance under that specific threat – no information is gained about the behaviour of the system more broadly. In order for a vulnerability analysis to be comprehensive, it is thus necessary to decouple the simulation of disruption scenarios from the hazards to which the system is exposed by using a comprehensive collection of disruption vectors.

### 3.4. Disruption Scenario Evaluation

The performance of the system in each scenario is the product of the performance function applied to that scenario:

$$Q: \boldsymbol{\Omega_{N-k}} \rightarrow \mathbb{R} \tag{3}$$

$$Q: \boldsymbol{\omega_i^{N-k}} \mapsto f[\boldsymbol{A}(\boldsymbol{\omega_i^{N-k}}), \boldsymbol{X_1}, \ldots, \boldsymbol{X_p}] \tag{4}$$

Each disruption scenario $\boldsymbol{\omega_i^{N-k}}$ is assigned, based on the performance function, a real number expressing the network performance in the new configuration. The real values representing the performance of the system in the different configurations are collected in an $N_k$–dimensional vulnerability vector $\boldsymbol{V^{N-k}}$. The performance of the system in the disruption scenario can then be treated as a discrete random variable, which associates a real number to each scenario $\boldsymbol{\omega_i^{N-k}}$, with the disruption space $\boldsymbol{\Omega_{N-k}}$ assuming the role of the sample space for this random variable. For ease of notation, the superscript *N-k* is hereafter dropped from $\boldsymbol{V^{N-k}}$.

# 4. VULNERABILITY COMPUTATION

## 4.1. A Distributional Metric

From the elements of the vulnerability vector a cumulative distribution function (CDF) *F* of the performance function *Q*, representing the system vulnerability to disruptions of order *k*, can be obtained:

$$F(v) = \frac{\sum_{i=i}^{N_k} I(V_i \leq v)}{N_k} \tag{5}$$

where $I(V_i \leq v) = 1$ if $V_i \leq v$ and 0 otherwise. This CDF is labelled here vulnerability distribution function, as it expresses the vulnerability of the system subject to disruptions of order *k*. It is bounded between 0 and 1, and it is non-decreasing. Analogously, a mass function can be defined:

$$f(v) = \frac{\sum_{i=i}^{N_k} I(V_i = v)}{N_k} \tag{6}$$

where $I(V_i = v) = 1$ if $V_i = v$ and 0 otherwise. The name vulnerability mass function will be used for this second entity.

For every *k*, the performance of the infrastructure varies between a minimum, corresponding to the worst-case scenario, and a maximum, depending on which of the network components are disrupted. Presenting the vulnerability of the infrastructure network in terms of a distribution allows for this variability to be captured and prevents any loss of information. The heterogeneity of the consequences is an important feature of the system performance and must be understood and actively managed: it is the key to reducing the uncertainty about future evolutions of system behaviour.

In order to summarise the characteristics of the vulnerability distribution, the vulnerability indicators are presented here. It is possible to use every indicator normally used in descriptive statistics to synthesise information about the characteristics of the vulnerability distribution, however, the following indicators are most useful.

1. The mean value of the vulnerability distribution $\mu$ informs the decision maker about the expected level of performance of a particular system given a specific disruption order:

$$\mu = \frac{1}{N_k} \sum_{i=1}^{N_k} V_i \tag{7}$$

2. The coefficient of variation $c_v$ of the vulnerability distribution provides information about its variability:

$$c_v = \frac{\sqrt{\frac{1}{N_k}\sum_{i=1}^{N_k}(V_i - \langle V \rangle)^2}}{\mu} \quad (8)$$

3. The kurtosis *K* accounts for peakedness of the distribution: when it is high, there is a sharp transition between a large number of standard, low-impact scenarios and a few extreme scenarios:

$$K = \frac{\frac{1}{N_k}\sum_{i=1}^{N_k}(V_i - \langle V \rangle)^4}{\left(\frac{1}{N_k}\sum_{i=1}^{N_k}(V_i - \langle V \rangle)^2\right)^2} - 3 \quad (9)$$

4. Vulnerability has also been presented as the proneness of a system to suffer disproportionate consequences from disruptive events (15) and this idea can be cast in terms of the constitutive elements of the vulnerability distribution. *D*, which is the ratio of a high quantile of the distribution (e.g. its 99.9$^{th}$ quantile) to the expected consequences, is used here as a measure of the disproportionateness of the consequences arising from the network configuration of the infrastructure:

$$D = \frac{V_{99.9}}{\mu} \quad (10)$$

## 4.2. Examples

The vulnerability analysis metric, Equation (5) described above, is applied here to networks of increasing complexity. In Section 4.2.1 theoretical network configurations are analysed – the purpose is to demonstrate the effectiveness of the vulnerability measures for different topologies, while Section 4.2.2 builds the vulnerability distribution for models of real infrastructure networks. In the examples below, $N-1$ scenarios are analysed ($N-k$ scenarios are addressed in Section 5.4) and connectivity loss $C_L$ is used as the performance function because it requires the least amount of further hypotheses on the networks. It is defined as:

$$C_L = 1 - \frac{n_c}{n} \quad (11)$$

where $n_c$ is the number of remaining nodes in the giant connected component and $n$ is the total number of nodes in the network. In the undisturbed configuration, $C_L = 0$. As is customary for numerical studies, the largest connected component of the network is used as a proxy for the giant connected component (50).

### *4.2.1. Theoretical Examples*

Vulnerability analyses have been carried on four example topologies, represented in Fig. 2, the star (Panel A), the tree (Panel B), the bat (Panel C) and the chain (Panel D). Descriptive statistics for the four networks are reported in Table III. The four example topologies have the same number of nodes (10 nodes) and a number of edges which varies from 9 (the minimum required to have a connected network) to 13. This corresponds to average degree in the range of 1.8 – 2.6, which is the case for many real-world infrastructure networks (54). Additionally, diameter (the largest distance among two nodes), efficiency (previously defined in Table II) and algebraic connectivity (the second largest eigenvalue of the Laplacian matrix) are reported in order to thoroughly characterise the example networks. Fig. 4 shows the histograms of the vulnerability mass functions of the four networks for $N-1$ scenarios, and Table IV reports the vulnerability indicators (represented by Equations (7)-(10)) used to synthesise the information.

The star and the chain network represent the two extremes. The star is highly vulnerable to the scenario which involves the central hub. While the mean value of vulnerability for the star network is not the highest, it is characterised by the largest value of the coefficient of variation, of the kurtosis and of the disproportionate consequences coefficient $D$. The chain does not present this variability across scenarios; the loss of any individual node has the same effect, in terms of connectivity. This leads to a vulnerability distribution which degenerates to a point value, zero coefficient of variation, indefinite kurtosis and a unitary value of coefficient $D$. The tree and the bat topologies represent intermediate examples: the maximum consequences of the removal of any individual node are respectively the loss of 70% and 60% of their connectivity. At the same time, however, between the most and the least severe scenarios there is for both networks an intermediate case. This leads to higher values of the mean, while the other three coefficients sit between those of examples A and D. The vulnerability analysis methodology presented here produces an assessment of the consequences of disruptive events which conveys all the information to the decision-maker: it allows for a comprehensive comparison among the performance of different network topologies, highlighting whether a specific configuration is sensitive to disruptions on average or in a few extreme cases and how much variability there is between the outcomes of different scenarios.

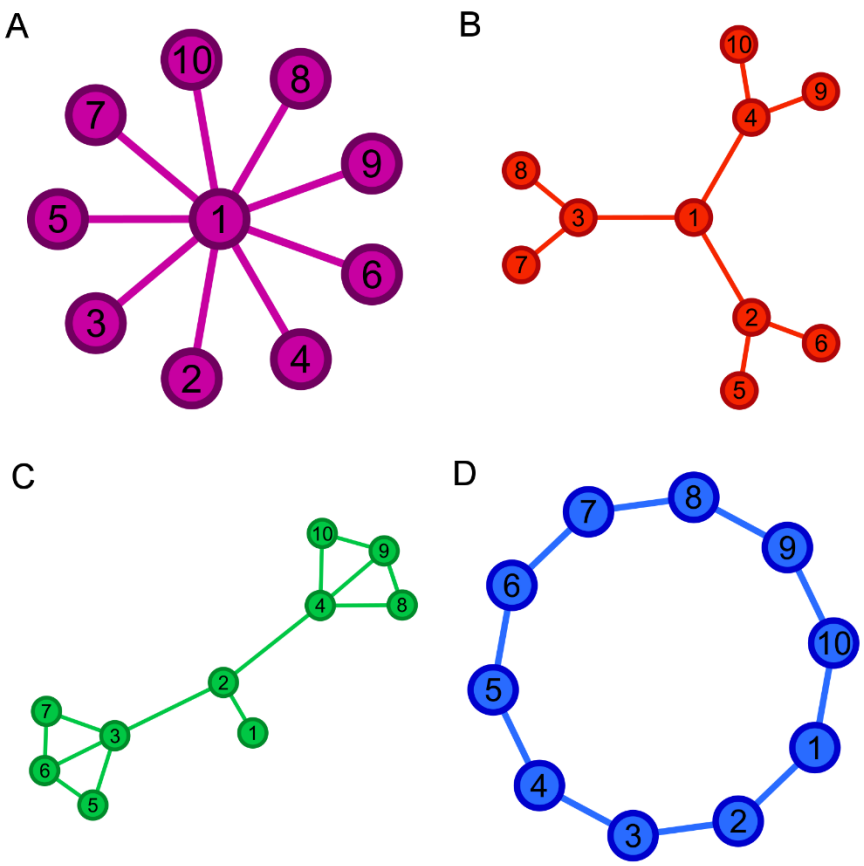


*Fig. 2. The four example topologies: the star (A), the tree (B), the bat (C) and the chain (D).*

*Table III: Topological features of the four example networks*

| | **A – Star** | **B – Tree** | **C – Bat** | **D – Chain** |
|---|---|---|---|---|
| Nodes | 10 | 10 | 10 | 10 |
| Edges | 9 | 9 | 13 | 10 |
| Average Degree | 1.8 | 1.8 | 2.6 | 2.0 |
| Diameter | 2 | 2 | 4 | 5 |
| Efficiency | 1.20 | 0.98 | 1.10 | 0.97 |
| Algebraic Connectivity | 1.00 | 0.27 | 0.21 | 0.38 |

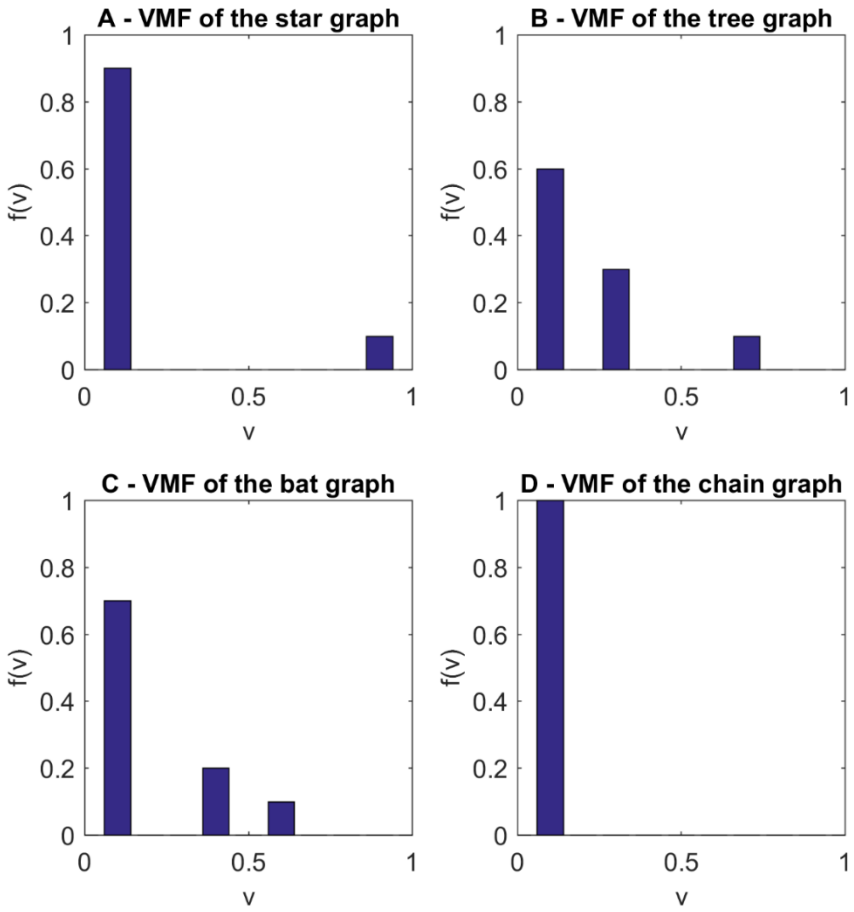


*Fig. 3. The Vulnerability Mass Function f(v) for the four example networks subject to N-1 scenarios.*

*Table IV. The Vulnerability Indicators calculated for the four example networks in Fig. 2 subject to N-1 scenarios*

| *Network* | *Mean* $\mu$ | *Coefficient of variation* $c_v$ | *Kurtosis* $K$ | *Disproportionateness* $D$ |
|---|---|---|---|---|
| A – Star | 0.18 | 1.41 | 8.11 | 5.00 |
| B – Tree | 0.22 | 0.87 | 4.82 | 3.18 |
| C – Bat | 0.21 | 0.88 | 2.80 | 2.86 |
| D – Chain | 0.10 | 0.00 | - | 1.00 |

### *4.2.2. Infrastructure Networks*

Three examples of infrastructure networks (Fig. 4) are analysed here. The first is the IEEE RTS96 Electric Power Transmission System (55). The second is the Great Britain Railway Network (GBRN), described in (56). The third

is the Colorado Springs Water Distribution Network (CSWN), introduced in (47). The size of the three networks spans across three orders of magnitude and their topological characteristics are summarised in Table V.

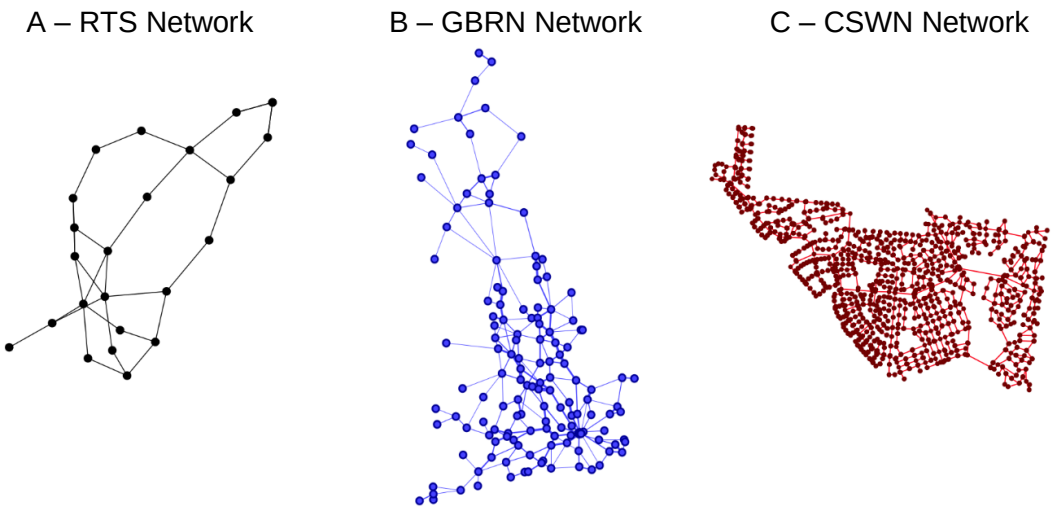


*Fig. 4. The three example infrastructure networks: the RTS (A), the GBRN (B) and the CSWN (C),*

*Table V: Topological features of the three example networks*

| | A – RTS | B – GBRN | C – CSWN |
|---|---|---|---|
| Nodes | 24 | 148 | 1786 |
| Edges | 34 | 270 | 1992 |
| Average Degree | 2.83 | 3.64 | 2.23 |
| Diameter | 7 | 22 | 569 |
| Efficiency | 0.8127 | 0.3916 | 0.1044 |
| Algebraic Connectivity | 0.1896 | 0.0246 | 0.0050 |

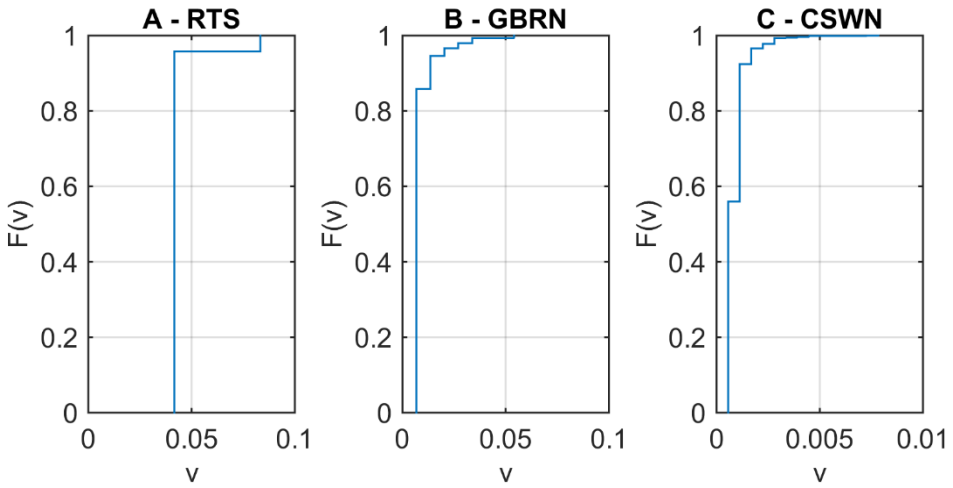


*Fig. 5. The vulnerability distributions F(v) of the three networks for N-1 scenarios: the RTS (A), the GBRN (B) and the CSWN (C),*

*Table VI. The Vulnerability Indicators for the three networks in Fig. 4 subject to N-1 scenarios*

| Network | $\mu$ | $c_v$ | $K$ | $D$ |
|---|---|---|---|---|
| A – RTS | 0.0434 | 0.1960 | 22.04 | 1.92 |
| B – GBRN | 0.0086 | 0.6908 | 29.90 | 6.30 |
| C – CWSN | 0.0009 | 0.6035 | 36.92 | 7.26 |

The results of an $N - 1$ vulnerability analysis are represented in Fig. 5 and synthesised by the vulnerability indicators in Table VI. All three networks have a meshed structure, typical of distribution networks: this yields a large fraction (96%, 86% and 56% respectively) of $N - 1$ scenarios which result only in the disconnection of the target node and no further consequences. The mean value of their vulnerability distributions is strongly dependent on the size of the network, which acts as a scaling parameter: there is approximately an order of magnitude difference between the three means. Examination of the other indicators shows scenario variability is lower on the RTS network (where only one node results in consequences other than its own disconnection), and comparable on the GBRN and CWSN systems. In the latter, however, high-consequence scenarios are more severe as compared to the average scenario (higher $D$ coefficient) and the transition is sharper (higher $K$).

The expected value of the vulnerability distribution, as observed here, is strongly size-dependent. As such, when two infrastructure networks of different sizes are to be compared, a normalisation of the mean based on the size of the network would be necessary in order to assess the relative magnitude of the $\mu$ indicator.

## 5. NOVELTIES OF THE PROPOSED METRIC

This approach allows for an improvement of the vulnerability analysis of infrastructure networks under three methodological perspectives, which are described below. First, it allows for a comparison with the outcome of a null model of network vulnerability, thus providing context to the significance of the analysis results. Second, it provides comprehensive information, overcoming the pitfalls of dealing with distributed systems. Finally, it can be readily used to assess the uncertainty that arises from the simulation of a sub-set of the scenarios in the disruption space.

## 5.1. Contextualisation of Information

When a vulnerability distribution is obtained, it is necessary to distinguish whether it arises from the specific network configuration or it is simply the result of having a system composed of interconnected elements. In other words, every network system will show a degradation in its performance if it is subject to the removal of its components: it is necessary to provide ranges for this inherent vulnerability in order to fully understand the behaviour of the network being disrupted. For this purpose, the use of a null model of vulnerability is advocated here. The aim of null models is to provide a reference against which to compare the properties of a specific network (57), and they are built using graphs which match one specific property of the network under investigation, but are otherwise random. In this case, the property being matched is the size of the network, in order to isolate its effects on the vulnerability of the system.

For an $N - k$ vulnerability analysis, the null model proposed here is the vulnerability envelope of the system. Given a network with $n$ nodes, $m$ edges and average degree $c = 2m / n$, a large number (e.g. $10^4$) of synthetic Erdős–Rényi (ER) random networks (58) is generated with the same number of nodes and average degree (in doing so, the primary purpose is to examine the behaviour of the distributional metric but it is recognised that many infrastructure networks grow out of the existing networks (59) and thus are not random). On each of these networks, a vulnerability analysis is performed, yielding a vulnerability distribution. The lower and upper envelopes of this ensemble of distributions provide bounds for how vulnerable a system of that specific size is expected to be. Fig. 7 shows the $N - 1$ vulnerability distribution previously obtained for the GBRN network with its vulnerability envelope. It is possible to notice that while the distribution sits within the envelope, it is very close to the upper bound, especially in the tail. This suggests that the GBRN system is more susceptible to disruptions than an average network of the same size and link density. Analytically, the comparison between the results is quantified using the vulnerability ratios.

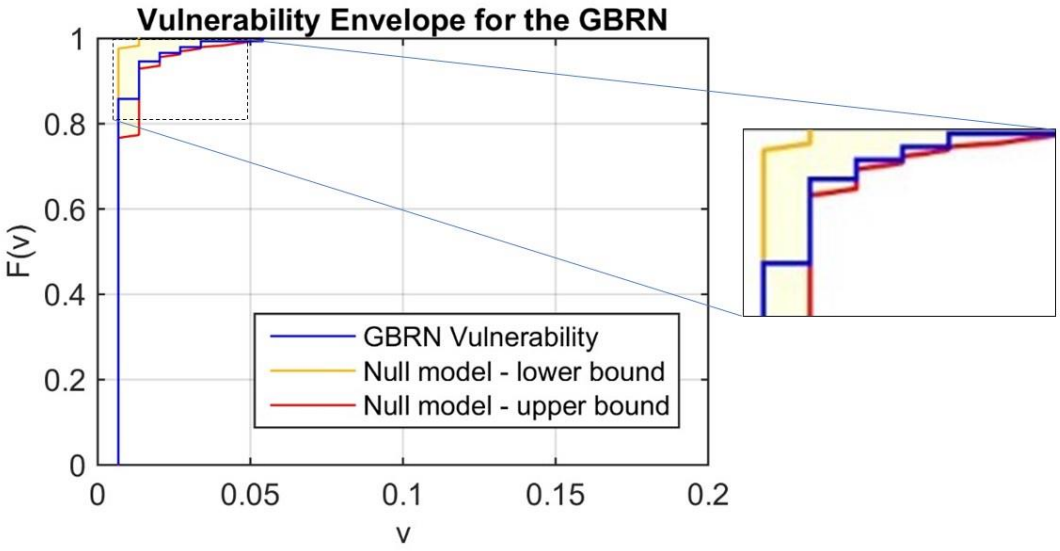


*Fig. 6. The vulnerability distribution of the GBRN network and the envelope obtained for it with ER networks with n = 148 and c = 3.64.*

*Table VII: Vulnerability indicators and vulnerability ratio obtained from the vulnerability distribution of the GBRN subject to N – 1 scenarios and a set of $10^4$ synthetic ER networks of the same size. For the ensemble of synthetic ER networks, the average value of each indicator and its 99-percentile are reported.*

| | **ER Networks** | | ***GBRN*** | |
|---|---|---|---|---|
| | $\langle VI_S \rangle$ | $VI_{S,99}$ | ***VI*** | ***R*** |
| **μ** | 0.0076 | 0.0089 | 0.0086 | 0.77 |
| $c_v$ | 0.3488 | 0.7056 | 0.6909 | 0.96 |
| ***K*** | 16.1419 | 56.1869 | 29.8085 | 0.34 |
| ***D*** | 2.9654 | 6.4355 | 6.2979 | 0.96 |

For each vulnerability indicator, the vulnerability ratio is defined as:

$$R = \max\left(\frac{VI - \langle VI_S \rangle}{VI_{S,99} - \langle VI_S \rangle}, 0\right) \tag{12}$$

where *VI* is the value of the vulnerability indicator on the network under scrutiny (e.g. the mean, or the coefficient of variation), $\langle VI_S \rangle$ is the expected value of the same indicator obtained by performing a numerical average over the indicators relative to the synthetic networks, and $VI_{S,99}$ is the 99$^{th}$ percentile of the indicator obtained from the sample of synthetic networks. The ensemble of ER networks is suitable from this perspective because their

generative model poses the least amount of assumptions on their structure and isolates the effects of size and edge density on the vulnerability of the system.

When $VI \leq \langle VI_S \rangle$, R = 0, vulnerability analysis shows that the system behaves how a network of the same size is expected to, or better. When $\langle VI_S \rangle < VI \leq VI_{S,99}$, $0 < R \leq 1$, the vulnerability indicator of the network for disruptions of the chosen size is on the high side of the sample of the synthetic networks, and as such its configuration may be critical and deserves further scrutiny. If $VI > VI_{S,99}$, R > 1, the network does worse than 99% of the synthetic networks, and therefore it is to be considered as critical and must be improved with topological interventions such as edge rewiring or creation of alternative hubs.

The GBRN network falls within the second regime (Table VII). Its vulnerability is worse than what is to be expected from the average networks of the same size but does not exceed the boundaries of the vulnerability envelope.

### 5.2. Completeness of Information

Section 4 has already shown how the use of the full vulnerability distribution produces a wealth of information about the sensitivity of the network to disruption scenarios. Here, it will be shown with an example that the use of the distribution is indeed necessary to avoid possible under- or over-representation of the network vulnerability arising from the use of its expected values (such as in (60), (61), or (62)).

The $N - 1$ vulnerability of networks generated with two such models, the Erdős–Rényi (ER) random network model and the Barabási–Albert (BA) scale-free network model (63), is examined here. Real-world infrastructure networks show topological properties in between those of the two models (54). As these models are stochastic in nature, 100 different networks were generated to capture the effect of minor topological changes on their performance. Vulnerability analysis is performed on each network, and Fig. 7 shows the envelope of the 100 different distributions. The point value of the vulnerability indicators reported in Table VIII is obtained by performing a numerical average of each indicator over all the 100 distributions; the table also reports the minimum and the maximum values of the four indicators attained over the 100 networks. In order for the results to be comparable, both models have been used to generate networks of 100 nodes, with a mean degree $\langle k \rangle = 2.70$ and initial connectivity $C = 1$.

*Table VIII. The Vulnerability Indicators calculated for the two models of networks (ER and BA) subject to N-1 scenarios*

| | $\mu$ | $c_v$ | $K$ | $D$ |
|---|---|---|---|---|
| A – ER Networks | 0.014 | 0.60 | 11.52 | 3.92 |
| [Min - Max] | [0.012 – 0.020] | [0.37 – 0.99] | [5.20 – 37.47] | [2.33 – 7.74] |
| B – BA Networks | 0.014 | 0.90 | 32.20 | 7.33 |
| [Min - Max] | [0.012 – 0.017] | [0.57 – 1.51] | [9.39 – 82.99] | [3.70 – 14.69] |

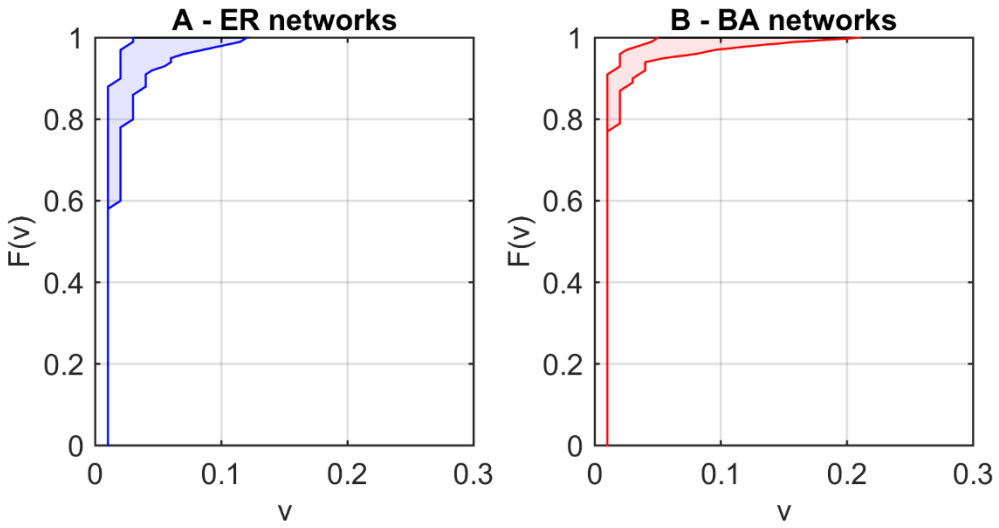


*Fig. 7. The envelopes of the Vulnerability Distribution Functions obtained with the two models of networks (ER and BA) subject to N-1 scenarios*

The $N$ – 1 vulnerability distributions of networks obtained with the two models are characterised by values of the mean falling in a similar range and with the same expected value (Table VIII). Their shape, however, is markedly different. This shows the shortcomings of approaches characterising vulnerability with a point value (5), such as the expected value of the consequences of $N$ – $k$ scenarios. In the examples, the expected value $\mu$ of $F(v)$ could lead to the incorrect conclusion that two classes of networks have the same vulnerability, while the BA networks are expected to be more susceptible to low-order disruptions, given their hub-and-spoke configuration. The vulnerability distributions show that this is the case (Table VIII): the BA networks have 50% higher variability in their response (highlighting greater unpredictability), higher kurtosis (pointing to the coexistence of different regimes of vulnerability) and higher values of the $D$ coefficient (indicating that extreme $N$ - 1 scenarios are more impactful as compared to ER networks).

### 5.3. Robustness of Information

For the examples presented so far, $N-1$ vulnerability analyses were performed. However, as the disruption order $k$ increases, there is an additional challenge: the number $N_k$ of scenarios in the disruption space increases with the binomial coefficient and it quickly becomes impossible to use a comprehensive set of scenarios to build the distribution. When this is the case, a sample $\boldsymbol{W_{N-k}}$ of the disruption space needs to be used, which is a set of $N_s$ distinct disruption scenarios of order $k$, with $N_s << N_k$, given the combinatorial explosion of $N_k$. The proposed approach allows for the quantification of the robustness of the information provided by vulnerability analysis by assessing the uncertainty arising from the use of $\boldsymbol{W_{N-k}}$. Rather than obtaining the exact $F$, an estimator $F_{Ns}$ can be obtained by treating the $N_s$ elements of the Vulnerability Vector $\boldsymbol{V}$ (obtained by evaluating scenarios in $\boldsymbol{W_{N-k}}$) as a sample of a random variable:

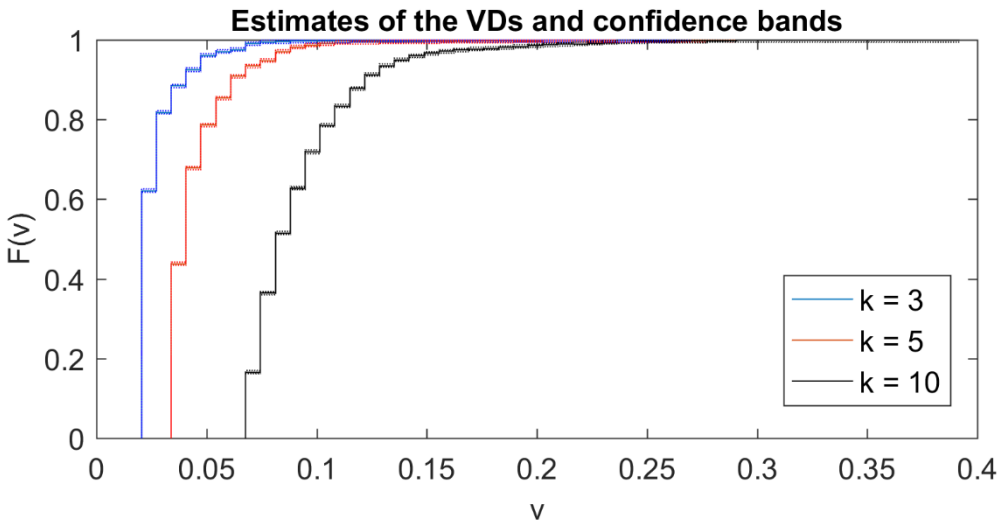


*Fig. 8. Estimates of the Vulnerability Distributions obtained for three disruption orders on the GBRN network and confidence bands.*

$$F_{N_s}(v) = \frac{\sum_{i=i}^{N_k} I(V_i \leq v)}{N_k} \tag{13}$$

where $I(V_i \leq v) = 1$ if $V_i \leq v$ and 0 otherwise. As the definition of the vulnerability distribution provided earlier mirrors that of a CDF, it is possible to build a 1 - $\alpha$ confidence band using methods such as the DKW inequality (64):

$$P(L(v) \leq F(v) \leq U(v) \ \ \forall v) \geq 1 - \alpha \tag{14}$$

where

$$L(v) = \max\left(\hat{F}_{N_s}(v) - \varepsilon_{N_s}, 0\right) \tag{15}$$

$$U(v) = \max\left(\hat{F}_{N_s}(v) + \varepsilon_{N_s}, 0\right) \quad (16)$$

and

$$\varepsilon_{N_s} = \sqrt{\frac{1}{2N_s} log \frac{2}{\alpha}} \quad (17)$$

In the above, $\alpha$ represents the likelihood that the real CDF does not fall within the confidence band and $\varepsilon_{Ns}$ is the half-width of the confidence band in terms of probability. The confidence band is narrow, e.g. for $\alpha = 10^{-2}$ and $N_s = 10^5$, $\varepsilon_{Ns} = 0.33 \times 10^{-2}$. Fig. 8 shows the 99.9% confidence band obtained using $N_s = 10^5$ scenarios for three selected disruption orders. The confidence interval does not depend on the cardinality of $\boldsymbol{\Omega_{N\text{-}k}}$: samples of constant size yield approximations of consistent quality for increasing disruption orders. The indicators obtained are also estimates of the true indicators, and their robustness can be tested with methods such as the bootstrap (65).

It should be noted that in the scientific literature, whenever simulation approaches are used to explore the vulnerability of infrastructure networks, they are accompanied by the caveat that only a limited portion of all the possible disruption scenarios are being sampled, (53, 66). However, the uncertainty associated with this selective sampling of scenarios has not been investigated previously. The analogy introduced earlier between the performance function and a random variable proves to be useful to quantify the uncertainty around the estimates of *F* yielded by simulations, where the stochastic process generating the uncertainty is the random sampling from $\boldsymbol{\Omega_{N\text{-}k}}$.

### 5.4. Example: the GBRN network

The GBRN network is examined here under $N - k$ scenarios involving node failures, for values of $k$ up to 75, (corresponding to 50% of the network nodes). Its performance under disruption scenarios is evaluated using the Connectivity function, as in the earlier exercise. The topological characteristics of the network are those reported in Table V. The number of independent scenarios sampled and evaluated for each disruption order $k$ is the maximum between $N_k$ and $N_s = 10^5$. $N_k$ becomes greater than $N_s$ already for $k = 3$: an exhaustive representation of the disruption space could be used only for $k = 1$ and $k = 2$. The results for all the disruption orders considered are represented by the box plots in Fig. 9 and the estimates of the indicators are plotted in Fig. 10.

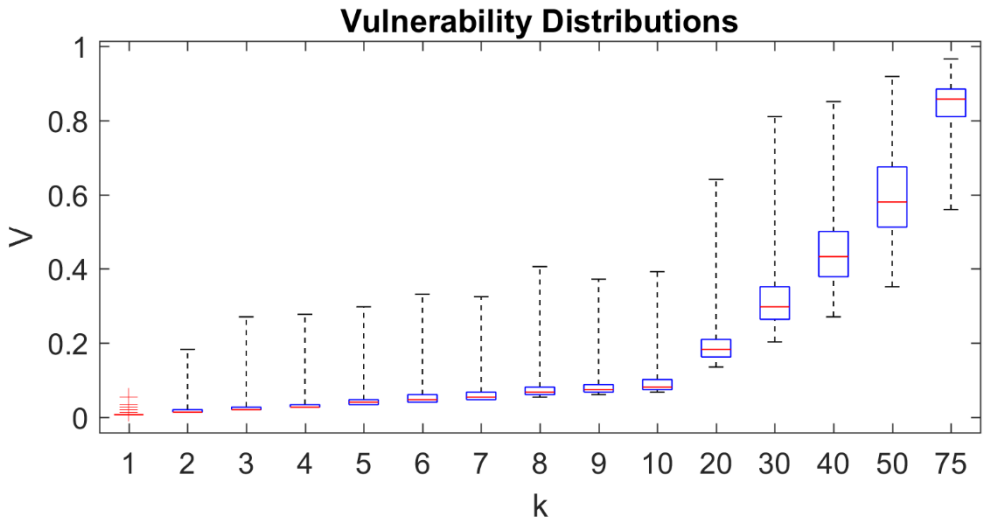


*Fig. 9. Minimum, 1st quartile, median, 3rd quartile and maximum of F obtained for different disruption orders k (N = 148) for GBRN network.*

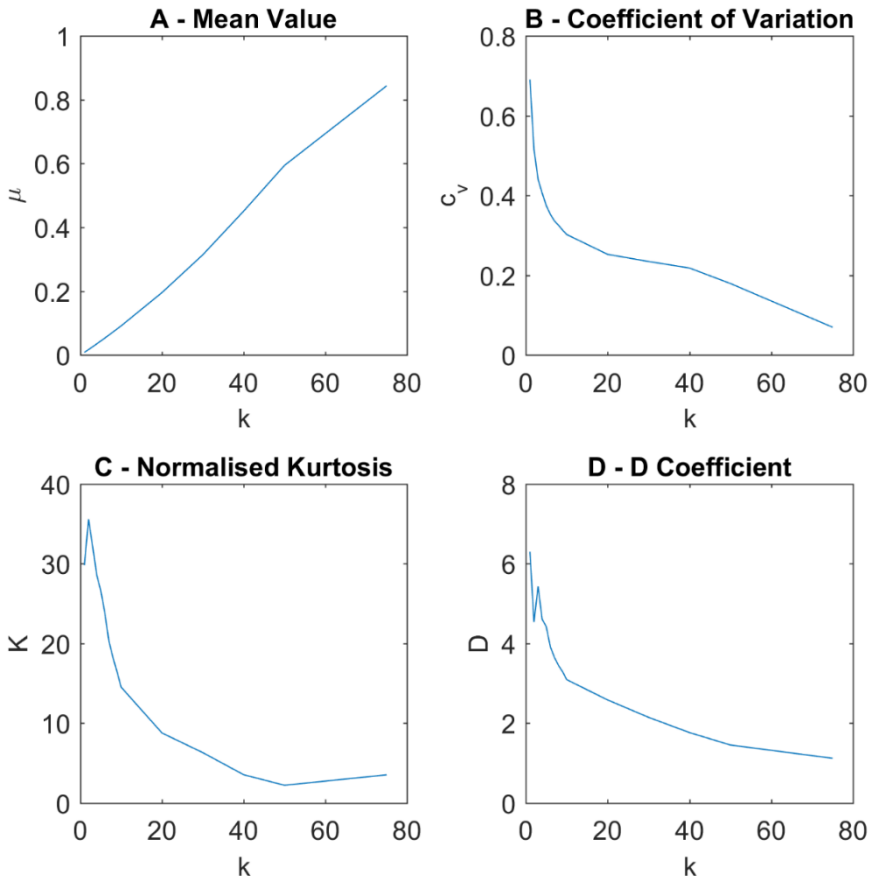


*Fig. 10. Evolution of the indicators of the vulnerability distributions with the disruption order k (N = 148) for GBRN network.*

Once again, it can be noted that using solely the expected value of the distribution to characterise the behaviour of the system would provide little information, as the $\mu$ scales almost linearly with the disruption order. The other indicators show more complex patterns, pointing to the shifting shape of the distribution shown in Fig. 9. What happens on this network is that higher order disruptions imply greater predictability coupled with larger values of the expected performance loss. As the damage, represented by k, increases in magnitude, its precise configuration matters progressively less, and the vulnerability distribution becomes more compact (decreasing $c_v$), less peaked (decreasing *K*) and less prone to suffer disproportionate consequences (decreasing *D*). The results suggest that the full vulnerability distribution should be used to manage the vulnerability of new infrastructure networks or modifications to the existing systems.

## 6. DISCUSSION

a) The vulnerability distribution metric provides a wealth of information about the behaviour of the networks subject to disruptions. The vulnerability metric indicators can be used as target functions for multi-objective optimisations of the system structure aimed at reducing specific aspects of their vulnerability. For example, an infrastructure showing high mean vulnerability values may need improvements across its whole structure, whereas another showing a high value of the *D* coefficient may need targeted improvement. Further, the evolution of vulnerability indicators over the disruption orders allows the decision-makers to assess whether the infrastructure shows sharp transitions into regions of higher vulnerability.

b) The proposed metric can also be used to identify whether the vulnerability is inherent in the size of the network or it is the results of its specific configuration. A procedure has been introduced for the creation of a null model for vulnerability. It is based on the use of an ensemble of synthetic ER networks aiming at capturing the effects of size and average connectivity. To the knowledge of the authors, this is the first time that such assessment has been put forward. Further, when assessing different infrastructure networks, average vulnerability values should not be relied upon, and instead vulnerability distributions should be used for a meaningful comparison among systems. Finally, the proposed metric allows for the quantification of the uncertainty around the estimates of vulnerability to high-order scenarios. No such quantification has been put forward in the literature, with the typical approach being the simulation of a certain number of scenarios, accompanied by the caveat that only a limited number of the possible system states is being explored (14).

c) Infrastructure networks are exposed to a wide variety of hazardous events for which the generative process is non-stationary (12) (67), but their performance is essential for the societies they support and they are therefore required to be robust to unforeseen events. Modelling disruptions as the removal of network elements eliminates the dependency of vulnerability analyses on the characteristics of specific disruption sources, leading to a hazard-independent analysis. At the same time, classifying disruptions by the number of affected elements facilitates a uniform comparison among events of the same magnitude, but involving the different system elements. This way, the proposed metric isolates the effects of the disruption order on the system performance, allowing the vulnerability of the infrastructure network to emerge.

d) The constituting elements of a vulnerability analysis framework have been identified clearly. This has enabled modifications of the individual components aimed at obtaining an exhaustive characterisation of the system performance and, at the same time, the recovery of various approaches used in the literature. For example, if multiple stakeholders are concerned with infrastructure performance, then any number of performance functions can be selected in Step 2 of the approach in order to perform multiple vulnerability analyses, each tailored to the needs of those stakeholders. If cascading failures can happen on the system under investigation (68), it means that a feedback loop exists between the performance function and the state of the elements, where the former dynamically influences the latter. Step 3 and Step 4 of the vulnerability analysis procedure have to be performed iteratively for every scenario until this feedback stabilizes, before computing the final performance of the network. Finally, the approach presented above only needs two minor modifications to account for spatial hazards (44): first, during Step 1 (the network modelling phase) each component must be assigned its geographical location and, second, the scenario selection performed in Step 3 has to be constrained to spatially-correlated sets of failures.

e) The procedure presented above is deterministic, but both the scenario generation phase and the performance functions can be cast in probabilistic terms. That is, a probability of failure can be assigned to each component and the interactions between them can be modelled as stochastic processes.
A modification of the scenario selection procedure of Step 3, accounting for the different likelihood of the network elements failing, would lead to the emergence of the risk-oriented approach typical of earthquake engineering and reliability analyses (36, 43, 69).

## 7. CONCLUSIONS

In this paper a framework for the vulnerability analysis of infrastructure networks has been formalised. For each disruption order, the approach is articulated in five phases, which are system modelling, selection of the performance model, selection of disruption scenarios, scenario evaluation and vulnerability computations. For the latter, a distributional metric has been proposed which is the main contribution of this paper. It presents several advantages over the existing vulnerability analysis methodologies.

First, the approach can be used to create a reference model for the results of a vulnerability analysis, in order to assess how much of the detected vulnerability derives from the specific configuration of the system under scrutiny. Second, by using the vulnerability distribution function and the indicators as the main output, the approach embraces the variability of the system performance which derives from the network configuration of the infrastructure. It was shown that doing otherwise, i.e. characterising vulnerability with a point value, may result in misleading conclusions. Third, the analogy established between the performance function and a random variable allows for a quantification of the uncertainty associated with simulations of samples of the disruption space. Finally, isolating the components of the vulnerability analysis allows for a transparent discussion around the analysis methodology and makes it clear how minor modifications of these components allow for the recovery of a number of other approaches used in the literature to assess the vulnerability of infrastructure networks.

Future research will examine specific applications of this approach. For example, decision-makers can be concerned with vulnerability at scales lower than the whole system. Also, the simulation of all scenarios independently of their geographical distribution may be considered too severe of a strain for the network to be assessed against and spatially-correlated failure scenarios will be explored. Further, the properties of different performance functions will be explored in order to assess their distribution on known topologies and establish reference distributions to compare the performance of infrastructure networks.

## Acknowledgements

The authors would like to thank the EPSRC (DTA Grant EP/L504919/1) and the Systems Centre at the University of Bristol, the EPSRC funded Industrial Doctorate Centre in Systems (Grant EP/G037353/1), for financial support to the first author.

## Declaration of interests

None

## REFERENCES


1. The Institution of Civil Engineers. The State of the Nation Infrastructure. 2014.
2. Zio E. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliab Eng Syst Saf. 2016;152:137–50.
3. Calderon C, Moral-Benito E, Serven L. Is Infrastructure Capital Productive? A Dynamic Heterogeneous Approach. J Appl Econom. 2015;30:177–98.
4. UNISDR. Sendai Framework for Disaster Risk Reduction 2015-2030. 2015.
5. SRA. Society of risk analysis, glossary of the specialty group on foundations of risk analysis. 2015. p. http://www.sra.org/news/sra-develops-glossary-risk.
6. Ouyang M, Mao Z, Yu M, Qi F, Hong L. A methodological approach to analyze vulnerability of interdependent infrastructure. Simul Model Pract Theory. 2009;17:12.
7. Su H, Zio E, Zhang J, Li X. A systematic framework of vulnerability analysis of natural gas pipeline network. Reliab Eng Syst Saf. 2018;175:79-91..
8. Johansson J, Hassel H. Impact of Functional Models in a Decision Context of Critical Infrastructure Vulnerability Reduction. Vulnerability, Uncertainty, Risk. 2014;577–86.
9. Bruneau M, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, Shinozuka M, et al. A framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthq Spectra. 2003;19(4):733–52.
10. Bush GW. Homeland Security Presidential Directive (HSPD-7): Critical infrastructure identification, prioritization, and protection. Retrieved from US Gov Print Off website http//www.gpo.gov. 2003;
11. UNISDR. Hyogo framework for action 2005-2015: building the resilience of nations and communities to disasters. In: Extract from the final report of the World Conference on Disaster Reduction (A/CONF 206/6). 2005.
12. Mulargia F. Why the Next Large Earthquake is Likely to be a Big Surprise. Bull Seismol Soc Am. 2013;103(5):2946–52.
13. Blockley D, Godfrey P, Agarwal J. Infrastructure resilience for high-impact low-chance risks. Proc Inst Civ Eng. 2012;165(Civil Engineering Special Issue):13–9.
14. Johansson J, Hassel H, Zio E. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. Reliab Eng Syst Saf. 2013;120:27–38.
15. Agarwal J, Blockley DI, Woodman NJ. Vulnerability of Systems. Civ Eng Environ Syst. 2001;18(2):141–65.
16. Fisher ME, Essam JW. Some Cluster Size and Percolation Problems. J Math Phys. 1961;2(4):609.
17. Cohen R, Erez K, Havlin S. Resilience of the Internet to Random Breakdowns. Phys Rev Lett. 2000;85:4626.
18. Callaway DS, Newman ME, Strogatz SH, Watts DJ. Network robustness and fragility: percolation on random graphs. Phys Rev Lett. 2000;85(25):5468–71.
19. Gao J, Buldyrev S V., Havlin S, Stanley HE. Robustness of a Network of Networks. Phys Rev Lett. 2010;107:195701.
20. Shao S, Huang X, Stanley HE, Havlin S. Percolation of localized attack on complex networks. New J Phys. 2015;17(2):23049.
21. Shinozuka M., Tanaka S. Effects of lifeline under seismic conditions. Paper 348, Eleventh World Conference on Earthquake Engineering. 1996.

22. Albert R, Jeong H, Barabasi A. Error and attack tolerance of complex networks. Nature. 2000;406(6794):378–82.

23. Pepyne DL. Topology and cascading line outages in power grids. J Syst Sci Syst Eng. 2007;16(2):202–21.

24. Crucitti P, Latora V, Marchiori M, Rapisarda A. Efficiency of scale-free networks: Error and attack tolerance. Phys A Stat Mech its Appl. 2003;320:622–42.

25. Ouyang M. Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. Chaos. 2013;23(2):23114.

26. Thacker S, Pant R, Hall J W. System-of-systems formulation and disruption analysis for multi-scale critical national infrastructures. Reliab Eng Syst Saf. 2017;167:30-41.

27. Anderson PL, Geckil IK. Northeast blackout likely to reduce US earnings by $6.4 billion [Internet]. 2003. Available from: http://www.andersoneconomicgroup.com/Portals/0/upload/Doc544.pdf

28. Nedic DP, Kirschen DS, Carreras BA, Lynch VE, Dobson I. Criticality in a cascading failure blackout model. Electr Power Energy Syst. 2006;28:7.

29. Motter A, Lai Y-C. Cascade-based attacks on complex networks. Phys Rev E. 2002;66(6):65102.

30. Zio E, Sansavini G. Modeling failure cascades in critical infrastructures with physically-characterized components and interdependencies. ESREL 2010 Annu Conf. 2010;651–2.

31. Dobson I, Carreras B a, Lynch VE, Newman DE. Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization. Chaos. 2007;17(2):26103.

32. Fang Y, Pedroni N, Zio E. Optimization of cascade-resilient electrical infrastructures and its validation by power flow modeling. Risk Anal. 2015;35(4):594–607.

33. Wilkinson SM, Dunn S, Ma S. The vulnerability of the European air traffic network to spatial hazards. Nat Hazards. 2011;60(3):1027–36.

34. Hong L, Ouyang M, Peeta S, He X, Yan Y. Vulnerability assessment and mitigation for the Chinese railway system under floods. Reliab Eng Syst Saf. 2015;137:58–68.

35. Dalziell E, Nicholson A. Risk and impact of natural hazards on a road network. J Transp Eng. 2001;127(April):159–66.

36. Poljansek K, Gutierrez E, Bono F. Seismic risk assessment of interdependent critical infrastructure systems: The case of European gas and electricity networks. Earthq Eng Struct Dyn. 2012;41:19.

37. Yazdani A., Otoo RA, Jeffrey P. Resilience-enhancing expansion strategies for water distribution systems: A network theory approach. Environ Model Softw. 2011;26:9.

38. Dunn S, Wilkinson SM. Identifying Critical Components in Infrastructure Networks Using Network Topology. ASCE J Infrastructure Systems. 2013;19(2):157–165.

39. Shuang Q, Zhang M, Yuan Y. Node vulnerability of water distribution networks under cascading failures. Reliab Eng Syst Saf. 2014;124:132–41.

40. Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliab Eng Syst Saf. 2014;121:18.

41. Johansson J., Hassel H. An approach for modeling interdependent infrastructures in the context of vulnerability analysis. Reliab Eng Syst Saf. 2010;95:1335–44.

42. Dueñas-Osorio L, Craig JI, Goodno BJ. Seismic response of critical interdependent networks. Earthq Eng Struct Dyn. 2007;36(September 2006):285–306.

43. Adachi T, Ellingwood B. Comparative assessment of civil infrastructure network performance under probabilistic and scenario earthquakes. J Infrastruct Syst. 2010;16(March):1–10.

44. Mensah AF, Dueñas-Osorio L. Efficient Resilience Assessment Framework for Electric Power Systems Affected by Hurricane Events. J Struct Eng. 2015; 142(8):1–10.

45. Matisziw TC, Murray AT, Grubesic TH. Exploring the vulnerability of network infrastructure to disruption.

Ann Reg Sci. 2008;43(2):307–21.

46. Dueñas-Osorio L, Vemuru SM. Cascading failures in complex infrastructure systems. Struct Saf. 2009;31(2):157–67.
47. Yazdani A, Jeffrey P. Complex network analysis of water distribution systems. Chaos. 2011;21(1):16111.
48. Rokneddin K, Ghosh J, Dueñas-Osorio L, Padgett JE. Bridge retrofit prioritisation for ageing transportation networks subject to seismic hazards. Struct Infrastruct Eng. 2013;9(10):1050–66.
49. Ouyang M, Zhao L, Hong L, Pan Z. Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability. Reliab Eng Syst Saf. 2014;123:38–46.
50. Newman MEJ. Networks: an introduction. Oxford: OUP; 2010.
51. Lorenz J, Battiston S, Schweitzer F. Systemic risk in a unifying framework for cascading processes on networks. Eur Phys J B. 2009;71(4):441–60.
52. Agarwal J. Blockley D. Liu M. A systems approach to vulnerability assessment. Proc Int Conf Vulnerability, Risk Anal Manag. 2011;
53. Murray AT, Grubesic TH, Matisziw TC. A Methodological Overview of Network Vulnerability Analysis. Growth Change. 2008;39(20):573.
54. Barthélemy M. Spatial networks. Phys Rep. Elsevier B.V.; 2011 Feb;499(1–3):1–101.
55. Grigg C, Wong P, Albrecht P, Allan R, Bhavaraju M, Chen Q. The IEE reliability test system - 1996 - Power Systems, IEEE Transactions on. IEEE Trans Power Syst. 1999;14(3):11.
56. Galvan G, Agarwal J. Community detection in action: identification of critical elements in infrastructure networks. ASCE Jnl Infrastructure Systems. 2018; 24(1):04017046.
57. Newman M, Girvan M. Finding and evaluating community structure in networks. Phys Rev E. 2004;69(2):26113.
58. Erdos P, Renyi A. On random graphs. Publ Math Debrecen. 1959;6:290–7.
59. Praks P, Kopustinskas V, Masera M. Probabilistic modelling of security of supply in gas networks and evaluation of new infrastructure. Reliab Eng Syst Saf. 2015; 144, 254–264.
60. Albert R, Albert I, Nakarado GL. Structural vulnerability of the North American power grid. Phys Rev E Stat Nonlin Soft Matter Phys. 2004;69(2 Pt 2):25103.
61. Dueñas-Osorio L, Goodno BJ, Craig JI, Bostrom A. Interdependent response of networked systems. J Infrastruct Syst. 2007;13(3):185–94.
62. Ouyang M. Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks. Reliab Eng Syst Saf. 2016;154:106–16.
63. Albert R, Barabasi A. Topology of evolving networks: local events and universality. Phys Rev Lett. 2000;85(24):5234–7.
64. Dvoretzky A, Kiefer J, Wolfowitz J. Asymptotic minimax character of the sample distribution function and of the classical multinomial estimator. Ann Math Stat. 1956;642–69.
65. Efron B, Tibshirani RJ. An introduction to the bootstrap. Chapman & Hall; 1993.
66. Johansson J, Hassel H, Zio E. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. Reliab Eng Syst Saf. 2013;120:27–38.
67. Allen MR, Barros VR, Broome J, Cramer W, Christ R, Church JA, et al. IPCC Fifth Assessment Synthesis Report-Climate Change 2014 Synthesis Report. 2014;
68. Zio E, Sansavini G. Component criticality in failure cascade processes of network systems. Risk Anal. 2011;31(8):1196–210.
69. Dueñas-Osorio L, Craig JI, Goodno BJ. Seismic response of critical interdependent networks. Earthq Eng Struct Dyn. 2007;36(September 2006):285–306.